(S//SI) Finding Genetic Sequences in SIGINT

FROM: [redacted]
Cryptanalysis Development Program Participant
Run Date: 12/08/2004

A cryptanalysis intern describes an unusual tour in Analysis & Production (S2). (U//FOUO)

(S//SI) The Office of Tradecraft for Analysis (S211A -- housed in the Advanced Analysis Lab) partners with other government agencies, academia, and private corporations to develop SIGINT analysis tradecraft and doctrine. OTA is made up of people with backgrounds ranging from analysis to engineering (and just about everything in between), working on problems related to how we do analysis. They address questions such as, "How can we best discover group structures and/or hierarchies from call graph metadata?" and "How do we identify unknown unknowns?" ... Practically speaking, what does that mean?

(S//SI) For a member of the Cryptanalysis Development Program (CADP), this means that OTA provides the unique opportunity to apply cryptanalytic skills to a significantly different problem set than that found in traditional CA tours. When I started my tour in the Lab, they were looking for someone to take on the problem of how to detect genetic sequences in SIGINT. The ultimate goals of this project are to gain general knowledge about genetic engineering research activity by foreign entities and to identify laboratories and/or individuals who may be involved in nefarious use of genetic research. As a signature of advanced laboratory activity and a strong indicator of the kind of research being peformed, the sequences are expected to lead us to that information.

(S//SI) I used many of the skills I learned in CA classes such as statistical analysis, and wrote several programs to test different algorithms, much like I had in my diagnosis tour. I also grew professionally by giving briefings to our customer and other interested groups, attending conferences (both in-house and external), and gaining a broader sense of the SIGINT system by partnering with another office. By teaming with the Technical Exploitation Center (TEC, S31123) we tested our most accurate algorithms in the front-end environment. This allowed us to identify the strengths and weaknesses of the algorithms that should be addressed in the final software product we implement in collection.

(U//FOUO) I thoroughly enjoyed my tour in OTA, and found it extremely rewarding to attack this unique problem with such success. To learn more about the Advanced Analysis Lab, see their home page , or type "go aal". For more information on the CA Development Program: "go CADP" or [redacted]